HAL open science

SMALL DOUBLING IMPLIES SMALL TRIPLING AT LARGE SCALES

Romain Tessera, Matthew Tointon

To cite this version:

Romain Tessera, Matthew Tointon. SMALL DOUBLING IMPLIES SMALL TRIPLING AT LARGE SCALES. 2023. hal-04315602

HAL Id: hal-04315602

https://hal.science/hal-04315602v1

Preprint submitted on 30 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

arXiv:2310.20500v1 [math.CO] 31 Oct 2023

SMALL DOUBLING IMPLIES SMALL TRIPLING AT LARGE SCALES

ROMAIN TESSERA AND MATTHEW TOINTON

Abstract. We show that if $K \geqslant 1$ is a parameter and S is a finite symmetric subset of a group containing the identity such $|S^{2n}| \leqslant K|S^n|$ for some integer $n \geqslant 2K^2$, then $|S^{3n}| \leqslant \exp(\exp(O(K^2)))|S^n|$. Such a result was previously known only under the stronger assumption that $|S^{2n+1}| \leqslant K|S^n|$. We prove similar results for locally compact groups and vertex-transitive graphs. We indicate some results in the structure theory of vertex-transitive graphs of polynomial growth whose hypotheses can be weakened as a result.

1. Introduction

The famous *Plünnecke–Ruzsa* inequalities state that if $K \geqslant 1$ is a parameter and A is a finite subset of an abelian group satisfying the *small doubling* hypothesis $|A + A| \leqslant K|A|$, then $|mA - nA| \leqslant K^{m+n}|A|$ for all non-negative integers m, n [5, 6, 7] (see also [4] for a dramatically simplified proof). It has long been known that the directly analogous statement fails for arbitrary non-abelian groups, and that a bound of the form $|A^2| \leqslant K|A|$ does not in general imply a bound of the form $|A^3| \leqslant O_K(|A|)$ (see e.g. [11, Example 2.5.2], which is essentially reproduced from [8]). Nonetheless, under the stronger *small tripling* assumption $|A^3| \leqslant K|A|$, we do have that $|A^{\epsilon_1} \cdots A^{\epsilon_m}| \leqslant K^{3(m-2)}|A|$ for all choices of $\epsilon_i = \pm 1$ and all $m \geqslant 3$ [11, Proposition 2.5.3]. A similar result holds more generally if A is an open precompact subset of a locally compact group, with Haar measure in place of cardinality [8, Lemma 3.4].

Breuillard and the second author showed that if A is a *ball* in a Cayley graph then the small-tripling hypothesis can *almost* be weakened to a small-doubling hypothesis, as follows.

Theorem 1.1 (Breuillard–Tointon [2, Lemma 2.10])**.** *Let $K \geqslant 1$. Suppose S is a finite symmetric subset of a group containing the identity, and $|S^{2n+1}| \leqslant K|S^n|$ for some $n \in \mathbb{N}$. Then $|S^{3n}| \leqslant O_K(|S^n|)$, and S^{2n} is an $O_K(1)$-approximate group.*

A *K-approximate group* is a symmetric subset A of a group containing the identity such that A^2 is covered by at most K left translates of A. The last conclusion of Theorem 1.1 is not stated in the reference, but follows immediately from the first conclusion and Lemma 2.1, below.

The purpose of the present note is to show that, at sufficiently large scales, a genuine small-doubling hypothesis is sufficient in Theorem 1.1, as follows.

Theorem 1.2. *Let $K \geqslant 1$. Suppose S is a finite symmetric subset of a group containing the identity, and $|S^{2n}| \leqslant K|S^n|$ for some integer $n \geqslant 2K^2$. Then $|S^{3n}| \leqslant \exp\exp(O(K^2)))|S^n|$, and S^{2n} is an $\exp(\exp(O(K^2)))$-approximate group.*

Moreover, we prove a similar result for locally compact groups, in which context nothing weaker than small tripling was previously known to suffice.

Theorem 1.3. *Given $K \geqslant 1$ there exists $n_0 = n_0(K) \ll K^{O(1)}$ such that if G is a locally compact group with Haar measure μ, and $S \subseteq G$ is a precompact symmetric open set containing the identity*

such that $\mu(S^{2n}) \leqslant K\mu(S^n)$ *for some integer* $n \geqslant n_0$*, then* $\mu(S^{3n}) \leqslant \exp(\exp(O(K^{O(1)})))\mu(S^n)$*, and* S^{2n} *is a precompact open* $\exp(\exp(O(K^{O(1)})))$*-approximate group.*

A particular reason to be interested in locally compact groups is that the automorphism group of a vertex-transitive graph Γ is a locally compact group with respect to the topology of pointwise convergence (see e.g. [9, §4] for details). Given a vertex $o \in \Gamma$, the set $S = \{g \in \mathrm{Aut}(\Gamma) : d(o, g(o)) \leqslant 1\}$ is a compact open generating set for $\mathrm{Aut}(\Gamma)$; moreover, if we write $\beta_\Gamma(n)$ for the number of vertices in a ball of radius n in Γ, and μ for the left Haar measure on $\mathrm{Aut}(\Gamma)$ normalised so that the stabiliser of o has measure 1, then we have $\beta_\Gamma(n) = \mu(S^n)$ for each $n \in \mathbb{N}$ [9, Lemma 4.8]. Theorem 1.3 therefore gives rise to the following corollary.

Corollary 1.4. *Given* $K \geqslant 1$ *there exists* $n_0 = n_0(K) \ll K^{O(1)}$ *such that if* Γ *is a locally finite vertex-transitive graph satisfying* $\beta_\Gamma(2n) \leqslant K\beta_\Gamma(n)$ *for some integer* $n \geqslant n_0$ *then* $\beta_\Gamma(3n) \leqslant \exp(\exp(O(K^{O(1)})))\beta_\Gamma(n)$*.*

To state the obvious, these results can immediately be implied to weaken the assumptions required in any result about groups or transitive graphs with a large-scale tripling bound amongst its hypotheses. Such results include the following, for example:

- Breuillard and the second author [2, Theorem 1.1] show that for all $K \geqslant 1$ there exist $n_0 = n_0(K)$ and $C = C(K) \geqslant 1$ such that if S is a symmetric subset of a group containing the identity, and $|S^{2n+1}| \leqslant K|S^n|$ for some integer $n \geqslant n_0$, then $|S^{rm}| \leqslant C^r|S^m|$ for all $r, m \in \mathbb{N}$ with $m \geqslant n$.
- Easo and Hutchcroft [3] have very recently proved a uniform version of the classical fact that a group of polynomial growth is finitely presented. To state their result formally, we borrow some terminology from their paper. Let G be a group with finite generating set S, so that $G \cong F_S/R$ for some normal subgroup R of the free group F_S. For each $n \in \mathbb{N}$, let R_n be the set of words of length at most 2^n in the free group F_S that are equal to the identity in G, and let $\langle R_n \rangle^{F_S}$ be the normal subgroup of F_S generated by R_n. Say that (G, S) has a *new relation on scale* n if $\langle R_{n+1} \rangle^{F_S} \neq \langle R_n \rangle^{F_S}$. Easo and Hutchcroft show that for each $K \geqslant 1$ there exist $n_0 = n_0(K) \in \mathbb{N}$ such that if G is a group and S is a finite symmetric generating set for G containing the identity and satisfying $|S^{3n}| \leqslant K|S^n|$ for some integer $n \geqslant n_0$ then
$$\#\Big\{m \in \mathbb{N} : m \geqslant \log_2 n \text{ and } (G, S) \text{ has a new relation on scale } m\Big\} \ll_{K,|S|} 1.$$
- Trofimov [12] has famously shown that an arbitrary vertex-transitive graph Γ of polynomial growth is quasi-isometric to a virtually nilpotent Cayley graph. In a previous paper of ours [9], we proved a finitary refinement of Trofimov's theorem [9, Theorem 2.3] under the hypothesis $\beta_\Gamma(3n) \leqslant K\beta_\Gamma(n)$.

Using either the non-abelian analogues of the Plünnecke–Ruzsa inequalities or the trivial observation that if A is a K-approximate group then $|A^m| \leqslant K^{m-1}|A|$, one can also easily bound the quantities $|S^{mn}|$, $\mu(S^{mn})$ or $\beta_\Gamma(mn)$ for $m > 3$ in the above results. However, in forthcoming work [10] we will provide much more precise bounds on these higher powers (in the case of Theorem 1.2, the result of Breuillard and the second author listed just above already improves upon this trivial extension).

2. Proofs

In this section we prove Theorems 1.2 and 1.3. We begin by noting that once we have bounded $|S^{3n}|$ or $\mu(S^{3n})$, the fact that S^2 is an approximate group follows immediately thanks to the following well-known result, which has its origins in the foundational paper [8] of Tao.

Lemma 2.1 ([9, Proposition 6.1])**.** *Let $K \geqslant 1$, and suppose A is a precompact symmetric open set in a locally compact group with a Haar measure μ. Suppose that $\mu(A^3) \leqslant K\mu(A)$. Then A^2 is a precompact open K^3-approximate group.*

In order to bound $|S^{3n}|$ or $\mu(S^{3n})$, we start by using the following results to show that S^n is covered by a few translates of some not-too-large approximate group U.

Proposition 2.2 (Tao [8, Theorem 4.6])**.** *Let $K \geqslant 1$, and suppose A is a precompact symmetric open set in a locally compact group with a Haar measure μ. Suppose that $\mu(A^2) \leqslant K\mu(A)$. Then there exists a precompact open $O(K^{O(1)})$-approximate group U with measure $\mu(U) \leqslant O(K^{O(1)})\mu(A)$ and a finite set X of cardinality at most $O(K^{O(1)})$ such that $A \subseteq XU$.*

Proposition 2.3 ([11, Theorem 2.5.6][1])**.** *Let $K \geqslant 1$, and suppose A is a finite subset of a group satisfying $|A^2| \leqslant K|A|$. Then there exists an $O(K^{18})$-approximate group $U \subseteq A^2$ and a set $X \subseteq A$ of size at most K^2 such that $A \subseteq XU$.*

The basic idea is then to show that the growth of S^n can be controlled in terms of the growth of U. We first refine U so that translates of it by distinct elements of X are strongly disjoint.

Lemma 2.4. *Suppose X and U are subsets of a group, with U symmetric and containing the identity and X finite. Then there exist $m \leqslant 5^{|X|-1}$ and $X' \subseteq X$ such that $x \notin yU^{4m}$ for all distinct $x, y \in X'$, and such that $XU \subseteq X'U^m$.*

Proof. If $x \notin yU^{4m}$ for all distinct $x, y \in X$, which in particular holds vacuously if $|X| = 1$, then we may take $m = 1$ and $X' = X$. We may therefore assume that there exist distinct $x, y \in X$ such that $x \in yU^{4m}$, and by induction that the lemma holds for all smaller sets X. The first of these assumptions implies in particular that $XU \subseteq (X \setminus \{x\})U^5$, and the induction hypothesis then implies that there exists $k \leqslant 5^{|X|-2}$ and $X' \subseteq X \setminus \{x\}$ such that $y \notin zU^{20k}$ for all distinct $y, z \in X'$, and such that $XU \subseteq (X \setminus \{x\})U^5 \subseteq X'U^{5k}$. We may therefore take this X', and $m = 5k$. □

One can think of Lemma 2.4 as saying that the translates xU^m of the approximate group U^m by elements $x \in X$ behave locally like cosets of a genuine subgroup. More precisely, given a subgroup H of a group G and elements $x, y \in G$, we trivially have $y \in xH$ if and only if $yH = xH$. The approximate group U^m given by Lemma 2.4 satisfies a 'local' version of this property, in that for all $x \in X$ and $y \in XU^m$, we have $y \in xU^m$ if and only if $yU^m \subseteq xU^{2m}$ and $xU^m \subseteq yU^{2m}$. The 'only if' direction of this is trivial. To prove the 'if' direction, first note that if $yU^m \subseteq xU^{2m}$ then

$$y \in xU^{3m}. \tag{2.1}$$

By definition there exists $z \in X$ such that $y \in zU^m$, but then combined with (2.1) and the conclusion of Lemma 2.4 this easily implies that $z = x$ and hence $y \in xU^m$.

The utility of this is that it allows us to prove a version of a rather useful property of the cosets of a genuine subgroup H of a group G with finite symmetric generating set S, namely that if H

[1]The reference states that U is an $O(K^{24})$-approximate group, but the proof there actually gives an $O(K^{18})$-approximate group.

has index bounded by $k \in \mathbb{N}$ then one may find a complete set of coset representatives for H inside S^{k-1}. This observation is crucial in Breuillard, Green and Tao's finitary refinement of Gromov's theorem [1, Corollary 11.2], for example. In our next result, which is the key new insight of the present work, we prove the following version of this in the setting in which we have a set of translates of a set U that are strongly disjoint in the sense of Lemma 2.4.

Proposition 2.5. *Let $k, n \in \mathbb{N}$. Suppose that S and U are symmetric subsets of a group, each containing the identity, and that X is a subset of size at most k such that $S^n \subseteq XU$ and $x \notin yU^4$ for all distinct $x, y \in X$. Then there exists $X' \subseteq S^{k-1}$ with $|X'| \leqslant |X|$ such that $S^n \subseteq X'U^2$.*

Proof. We may assume that X is minimal such that $S^n \subseteq XU$. For each $r = 0, 1, \ldots, n$, define $X_r = \{x \in X : xU \cap S^r \neq \varnothing\}$, noting that $X_n = X$ by minimality of X.

We claim that if $X_{r+1} = X_r$ for some $r \leqslant n-2$ then $X_{r+2} = X_{r+1}$. To see this, suppose that $X_{r+1} = X_r$, and let $x \in X_{r+2}$. By definition, this means that there exists $u \in U$ such that $xu \in S^{r+2}$. This in turn implies that there exists $s \in S$ such that $xu \in sS^{r+1} \subseteq sX_{r+1}U = sX_rU$. It follows that there exist $y \in X_r$ and $v \in U$ such that $xu = syv$. By definition of X_r, there exists $w \in U$ such that $yw \in S^r$. It then follows that $syw \in S^{r+1}$, hence $xu = syv \in S^{r+1}U^2$, and hence $x \in S^{r+1}U^3 \subseteq X_{r+1}U^4$. By hypothesis, it then follows that $x \in X_{r+1}$ as claimed.

By induction, this claim implies that if $X_{r+1} = X_r$ for some $r < n$ then $X_r = X_n = X$. Since $|X_0| \geqslant 1$, it follows that if $k \leqslant n$ then $X_{k-1} = X$. Combined with the fact that $X_n = X$, this implies in all cases that for each $x \in X$ there exists $x' \in S^{k-1}$ such that $x' \in xU$, and hence $xU \subseteq x'U^2$ by symmetry of U. Setting $X' = \{x' : x \in X\}$, we therefore have $X' \subseteq S^{k-1}$, $|X'| \leqslant |X|$ and $S^n \subseteq XU \subseteq X'U^2$ as required. □

The next lemma shows that if X is contained in a ball of small enough radius in S and $S^n \subseteq XU$ then the further growth of S is controlled by the growth of U.

Lemma 2.6. *Let $k, r \in \mathbb{N}$. Suppose G is a group with symmetric generating set S containing the identity, and $X \subseteq S^k$ and $U \subseteq G$ satisfy $S^{r+k} \subseteq XU$. Then $S^{mr+k} \subseteq XU^m$ for all $m \in \mathbb{N}$.*

Proof. The case $m = 1$ is true by hypothesis, and for $m > 1$ by induction we have $S^{mr+k} = S^r S^{(m-1)r+k} \subseteq S^r XU^{m-1} \subseteq S^{r+k}U^{m-1} \subseteq XU^m$, as required. □

Proof of Theorems 1.2 and 1.3. We will prove Theorem 1.2 in detail; the proof of Theorem 1.3 is identical, but with Proposition 2.2 in place of Proposition 2.3 right at the start and Haar measure in place of cardinality where appropriate. Proposition 2.3 implies that there exists an $O(K^{18})$-approximate group $U \subseteq S^{2n}$ and a set $X \subseteq S^n$ of size at most K^2 such that $S^n \subseteq XU$. Lemma 2.4 then implies that there exist $m \leqslant 5^{K^2}$ and $X' \subseteq X$ such that $x \notin yU^{4m}$ for all distinct $x, y \in X'$, and such that $S^n \subseteq X'U^m$. Proposition 2.5 then implies that there exists $X'' \subseteq S^{K^2-1} \subseteq S^{\lfloor n/2 \rfloor}$ with $|X''| \leqslant K^2$ such that $S^n \subseteq X''U^{2 \cdot 5^{K^2}}$. Applying Lemma 2.6 with $k = \lfloor n/2 \rfloor$ and $r = \lceil n/2 \rceil$ then implies that $S^{3n} \subseteq X''U^{10 \cdot 5^{K^2}}$, and hence that $|S^{3n}| \leqslant |X''| K^{O(5^{K^2})} |U| \leqslant K^{O(5^{K^2})} |S^n| \leqslant \exp(\exp(O(K^2)))|S^n|$, as required. The fact that S^{2n} is an $\exp(\exp(O(K^2)))$-approximate group then follows from Lemma 2.1. □

References

[1] E. Breuillard, B. J. Green and T. C. Tao. The structure of approximate groups, *Publ. Math. IHES.* **116**(1) (2012), 115–221.

[2] E. Breuillard and M. C. H. Tointon. Nilprogressions and groups with moderate growth, *Adv. Math.* **289** (2016), 1008–1055.

[3] P. Easo and T. Hutchcroft. Uniform finite presentation for groups of polynomial growth, arXiv:2308.12428.
[4] G. Petridis, New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, **32**(6) (2012), 721–733.
[5] H. Plünnecke, Eine zahlentheoretische Anwendung der Graphentheorie. *J. Reine Angew. Math.*, **243** (1970), 171–183.
[6] I. Z. Ruzsa, An application of graph theory to additive number theory. *Scientia, Ser. A*, **3** (1989), 97–109.
[7] I. Z. Ruzsa, Addendum to: An application of graph theory to additive number theory. *Scientia, Ser. A*, **4** (1990/91), 93–94.
[8] T. C. Tao. Product set estimates for non-commutative groups, *Combinatorica* **28**(5) (2008), 547–594.
[9] R. Tessera and M. C. H. Tointon. A finitary structure theorem for vertex-transitive graphs with polynomial growth. *Combinatorica* **41**(2) (2021), 263–298.
[10] R. Tessera and M. C. H. Tointon. Balls in groups: volume, structure and growth. In final preparation.
[11] M. C. H. Tointon. *Introduction to approximate groups*, London Mathematical Society Student Texts **94**, Cambridge University Press, Cambridge (2020).
[12] V. I. Trofimov. Graphs with polynomial growth, *Math. USSR-Sb.* **51** (1985) 405–417.

Institut de Mathématiques de Jussieu-Paris Rive Gauche, France
Email address: romain.tessera@imj-prg.fr

School of Mathematics, University of Bristol, United Kingdom
Email address: m.tointon@bristol.ac.uk